UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/786,224 | 02/26/2004 | Burkhard Kuhls | 080437.53236US | 2832 |

23911 7590 06/01/2007

CROWELL & MORING LLP
INTELLECTUAL PROPERTY GROUP
P.O. BOX 14300
WASHINGTON, DC 20044-4300

| EXAMINER | |
|---|---|
| JOHNSON, CARLTON | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/01/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/786,224 | KUHLS, BURKHARD | |
| | Examiner | Art Unit | |
| | Carlton V. Johnson | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *26 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2-26-2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is responding to application papers filed on **2-26-2004**.

2. Claims **1 - 18** are pending. Claim **1** is independent.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim **1 - 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wong** (US Patent No. **5,957,985**) in view of **Drews et al.** (US Patent No. **6,463,535**).

**Regarding Claim 1**, Wong discloses:

a method comprising providing software for use by a control unit of a vehicle, (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit) Wong does not specifically disclose signing the software against falsification, using a secret or private key of a software signature site, and checking the signed software for integrity.

However, Drews discloses:

a) before its use by the control unit, signing the software against falsification, using a secret or private key of a software signature site, according to a public-key

method; (see Drews col. 1, lines 62-67: pre-boot software, before use by local platform (control unit); col. 4, lines 48-54: sign software; utilizing private key, PKI technique; col. 2, lines 48-51: software download) and

b) checking the signed software for integrity, using a public key complementary to the secret key of the software signature site. (see Wong col. 4, lines 1-6; col. 4, lines 9-14; col. 4, lines 23-26: verify (check) signature with public key (complimentary to private (secret) key), validity check)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for signing the software against falsification, and checking the signed software for integrity. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59: " *... Unfortunately, there is currently no security scheme to ensure the integrity of the boot image (e.g., check that the software is free from viruses or has not been tampered with before or during download) as well as its authenticity (e.g., check that the boot image originated from its proper source). The present invention provides a scheme that overcomes these security flaws. ...* ")

**Regarding Claim 2**, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: vehicle control unit) Wong does not specifically disclose generating a software signature certificate, using the public key of the software signature site and a secret key of a control entity. However, Drews

discloses wherein further comprising generating a software signature certificate, using the public key of the software signature site and a secret key of a control entity, of a trust center, according to a public-key method. (see Drews col. 4, lines 48-54: signature generated; col. 4, lines 15-18; col. 4, lines 20-23: digital certificate for software)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability to generate a software signature certificate, using the public key of the software signature site and a secret key of a control entity, using a secret or private key of a software signature site, and checking the signed software for integrity. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 3**, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: vehicle control unit) Wong does not specifically disclose a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity. However, Drews discloses wherein one of a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity. (see Wong col. 4, lines 26-30: authorization certificate(s), trust center (manufacturer), and control (local platform); col. 4, lines 48-54: sign using private (secret) key)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 4**, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: vehicle control unit) Wong does not specifically disclose clearing code data are signed using a secret key of a clearing code site according to a public key method. However, Drews discloses wherein clearing code data are signed using a secret key of a clearing code site according to a public key method. (see Drews col. 4, lines 48-54: software (clearing code) signed using private (secret) key of manufacturer)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for clearing code data are signed using a secret key of a clearing code site according to a public key method. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 5**, Wong discloses the method according to claim 2. (see Wong col.

2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not disclose a clearing code site signature certificate is generated using the secret key of the control entity of the trust center according to a public-key method. However, Drews discloses wherein a clearing code site signature certificate is generated using the secret key of the control entity of the trust center according to a public-key method. (see Drews col. 4, lines 26-30: multiple authorization certificates, manufacture (trust center), and local platform (control unit))

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for the clearing code site signature certificate to be generated using the secret key of the control entity of the trust center according to a public-key method. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 6**, Wong discloses the method according to claim 3. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit. However, Drews discloses wherein the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit. (see Drews col. 3, lines 50-63: protected storage (memory, write restricted))

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 7**, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the clearing code site signature certificate, the software signature certificate, the clearing code data and their signature as well as the software and its signature are stored in the control unit. However, Drews discloses wherein the clearing code site signature certificate, the software signature certificate, the clearing code data and their signature as well as the software and its signature are stored in the control unit. (see Drews col. 4, lines 26-30: certificate (public key) stored in persistent storage, local platform (control unit); col. 3, lines 50-63: software stored in local platform (control unit) memory; col. 4, lines 26-30: multiple certificates, (clearing code, trust center, manufacturer))

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews for the clearing code site signature certificate, the software signature certificate, the clearing code data and their signature as well as the software and its signature are stored in the control unit. One of ordinary skill in the art would have been

motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 8**, Wong discloses the method according to claim 2. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose software signature certificate includes at least one validity restriction. However, Drews discloses wherein the software signature certificate includes at least one validity restriction. (see Drews col. 4, lines 9-14: boot image provided by acceptable source (validity restriction))

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for a software signature certificate including at least one validity restriction. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 9**, Wong discloses the method according to claim 5. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to a vehicle identification number of a particular vehicle. However, Drews

discloses wherein the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to a vehicle identification number of a particular vehicle. (see Drews col. 2, line 59 - col. 3, line 3: serial number linked to manufacturer; col. 3, lines 50-63: write protected storage area; col. 4, lines 9-14: validity restriction)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to a vehicle identification number of a particular vehicle. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 10**, Wong discloses the method according to claim 2. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the software signature certificate is checked for integrity according to a public-key method, using a public key of the trust center. However, Drews discloses wherein the software signature certificate is checked for integrity according to a public-key method, using a public key of the trust center. (see Drews col. 2, lines 59-

66: public key techniques; col. 4, lines 20-23: trust center, provide software; col. 2, lines 32-35; col. 4, lines 1-6: verify (integrity check))

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability for the software signature certificate is checked for integrity according to a public-key method, using a public key of the trust center. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 11**, Wong discloses the method according to claim 2. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the signed software is checked for integrity according to a public key method, using the public key of the software signature site contained in the software signature certificate. However, Drews discloses wherein the signed software is checked for integrity according to a public key method, using the public key of the software signature site contained in the software signature certificate. (see Drews col. 2, lines 32-35; col. 5, lines 46-49: integrity checked, public key utilized)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability that the signed software is checked for integrity according to a public key method, using the public key of the software signature site contained in the software signature certificate. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability

to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 12**, Wong discloses the method according to claim 5. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center. However, Drews discloses wherein the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center. (see Drews col. 2, lines 59-66: public key techniques; col. 2, lines 32-35; col. 4, lines 9-14: verify (integrity check), software from trusted source)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews to enable the capability whereby the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 13**, Wong discloses the method according to claim 4. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the signed clearing code data are checked for integrity according to a public key method, using a public key of the clearing code site contained in the

clearing code site signature certificate. However, Drews discloses wherein the signed clearing code data are checked for integrity according to a public key method, using a public key of the clearing code site contained in the clearing code site signature certificate. (see Drews col. 2, lines 57-67: public key within certificate; col. 2, lines 32-35; col. 4, lines 9-14: verify (integrity check) utilizing public key in certificate)

It would have been obvious to one of ordinary skill in the art to modify Wong as taught by Drews for the signed clearing code data are checked for integrity according to a public key method. One of ordinary skill in the art would have been motivated to employ the teachings of Drews in order to enable the capability to ensure the integrity and authenticity of a software image before execution. (see Drews col. 1, lines 53-59)

**Regarding Claim 14**, Wong discloses the method according to claim 1, wherein the control unit is equipped with a sequence-controlled microprocessor that implements one of the above-described methods. (see Wong col. 2, lines 21-29: vehicle processor (microprocessor))

**Regarding Claim 15**, Wong discloses a control unit for a motor vehicle, which implements a method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: control unit, vehicle)

**Regarding Claim 16**, Wong discloses a data processing system for a motor vehicle, which implements a method according to claim 1. (see Wong col. 4, line 64 - col. 5, line

8; col. 7, lines 35-39: computer, data processing system)

**Regarding Claim 17**, Wong discloses a computer program product sequence control of a data processing system of a motor vehicle or motorcycle, which implements the method according to claim 1. (see Wong col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: computer, data processing system, vehicle)

**Regarding Claim 18**, Wong discloses a data carrier, comprising a computer program product according to claim 17. (see Wong col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software (computer program product) implementation means)

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

C.J.

CVJ
May 14, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

5/27/07